Amendments to the Claims:

Please amend claims 25-29.
Please cancel claims 1-9 and 14-19, without prejudice.

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. – 9. (Cancelled)

10. (Previously Presented) An agent embodied in a computer-readable medium for use in a system for performing penetration testing of a target computer network having a target host, the agent comprising:

a system-calls proxy server configured to receive and execute, in the target host, system calls received via a network; and

a virtual machine configured to execute, in the target host, scripting language instructions received via the network,

wherein the system calls received via the network are routed to the system-calls proxy server and the scripting language instructions received via the network are routed to the virtual machine.

11. (Previously Presented) The agent of claim 10, further comprising an execution engine configured to control the system-calls proxy server and the virtual

machine, wherein the system calls and the scripting language instructions are routed to the system-calls proxy server and the virtual machine, respectively, by the execution engine.

12. (Original) The agent of claim 11, further comprising a remote procedure call module configured to receive commands from the network formatted in a remote procedure call protocol and pass the commands to the execution engine.

13. (Previously Presented) An agent embodied in a computer-readable medium for use in a system for performing penetration testing of a target computer network, having a target host, the agent comprising:

a system-calls proxy server configured to receive and execute, in the target host system calls received via a network;

a virtual machine configured to execute, in the target host, scripting language instructions received via the network;

a secure communication module configured to provide secure communication between the virtual machine and the network;

an execution engine configured to control the system-calls proxy server and the virtual machine, wherein the system calls and the scripting language instructions are routed to the system-calls proxy server and the virtual machine, respectively, by the execution engine;

a remote procedure call module configured to receive commands via the network formatted in a remote procedure call protocol and pass the commands to the execution engine; and

a second secure communication module configured to provide secure communication between the remote procedure call module and the network.

14. – 19. (Cancelled)

20. (Previously Presented) A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

sending a system call to the first remote agent via a network; and

executing the system call in the first target host using a system-calls proxy server of the first remote agent to exploit a security vulnerability of a second target host,.

wherein the system call comprises a computer instruction that is executed in an operating system of the first target host.

21. (Previously Presented) A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing in the first remote agent a second module that generates a system call; and

executing the system call in the first target host to exploit a security vulnerability of a second target host,

wherein the system call comprises a computer instruction that is executed in an operating system of the first target host.

22. (Previously Presented) A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing a second module in the first remote agent that generates a system call;

installing a second remote agent in a second target host as a result of exploiting a security vulnerability of the second target host;

sending the system call generated by the second module to the second remote agent via a network; and

executing the system call in the second target host using a system-calls proxy server of the second remote agent,

wherein the system call comprises a computer instruction that is executed in an operating system of the second target host.

23. (Previously Presented) A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending a system call to the first remote agent;

sending the system call from the first remote agent to the second remote agent; and

executing the system call in the second target host using a system-calls proxy server of the second remote agent,

wherein the system call comprises a computer instruction that is executed in an operating system of the second target host.

24. (Previously Presented) A method for performing penetration testing of a target network, comprising the steps of:

installing a first remote agent in a first target host of the target network, the first remote agent having a system-calls proxy server configured to receive and execute system calls;

executing in the first remote agent a system call received via a network, the system call comprising a computer instruction that is executed in an operating system of the first target host;

installing a second remote agent in the first target host, the second remote agent having a system-calls proxy server configured to receive and execute system calls and a virtual machine configured to execute scripting language instructions; and

executing in the second remote agent a scripting language instruction or a system call received via the network.

25. (Currently Amended) Computer code embodied in a computer readable medium for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

sending a system call to the first remote agent via a network; and

executing the system call in the first target host using a system-calls proxy server of the first remote agent to exploit a security vulnerability of a second target host, the

system call comprising a computer instruction that is executed in an operating system of the first target host.

26. (Currently Amended) Computer code embodied in a computer readable medium for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing in the first remote agent a second module that generates a system call; and

executing the system call in the first target host to exploit a security vulnerability of a second target host, the system call comprising a computer instruction that is executed in an operating system of the first target host.

27. (Currently Amended) Computer code embodied in a computer readable medium for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing a second module in the first remote agent that generates a system call;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending the system call generated by the second module to the second remote agent via a network; and

executing the system call in the second target host using a system-calls proxy server of the second remote agent, the system call comprising a computer instruction that is executed in an operating system of the second target host.

28. (Currently Amended) Computer code embodied in a computer readable medium for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending a system call to the first remote agent;

sending the system call from the first remote agent to the second remote agent; and

executing the system call in the second target host using a system-calls proxy server of the second remote agent, the system call comprising a computer instruction that is executed in an operating system of the second target host.

29. (Currently Amended) Computer code embodied in a computer readable medium for performing penetration testing of a target network, the code comprising code for:

installing a first remote agent in the first target host, the first remote agent having a system-calls proxy server configured to receive and execute system calls;

executing in the first remote agent a system call received via a network, the system call comprising a computer instruction that is executed in an operating system of the first target host;

installing a second remote agent in the first target host, the second remote agent having a system-calls proxy server configured to receive and execute system calls and a virtual machine configured to execute scripting language instructions; and

executing in the second remote agent a scripting language instruction or a system call received via the network.